AU/ACSC/053/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

GLOBALIZATION

AND ASYMMETRICAL WARFARE

by

William J. Hartman, Major, US Army

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Paul R. Kan

Maxwell Air Force Base, Alabama

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 APR 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Globalization And Asymmetrical Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**52**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

This research paper analyzes the globalization trend and the effect it is having on the ability to conduct asymmetrical attacks against the United States and our Allies worldwide. This research is intended to provide insight into the way that globalization is allowing our potential adversaries to act on a global scale. Recommendations on force structure and policy changes are intended to provide options to ensure we are better prepared for the future threat. I would like to thank Dr, Paul Kan for his guidance and direction on this project. I would also like to thank the staff at the Air University Library and the National Defense Research Institute Report (Rand) for providing research assistance on the project.

AU/SCHOOL/053/2001-04

Abstract

Globalization is having a tremendous effect on the ability of terrorist and criminal organizations to act on a global scale. These organizations are using asymmetrical means to target U.S. interests at home and abroad. The events of September 11th were the culminating effect of this trend that has played an increasingly greater role in the world in which we live. This research paper analyzes the globalization trend and the effect it is having on the ability to wage this new type of war. The negative effects of globalization have continued to create a large disenfranchised population primarily centered in the Middle East, Africa, and Asia. This disenfranchised population has become the recruitment pool and their countries have become training bases for the networked terrorist and criminal who take advantage of the tools of globalization. Those tools include the internet that provides secure means of communication, the technology that enables them to act, and the porous environment that allows one to move around the world undetected. The U.S. needs to develop a better National Security Structure to deal with this threat and solve longstanding foreign policy issues. This security structure would take advantage of a network architecture that would be much more suited to managing information which is the primary weapon in the globally connected world. Policy changes would address issues that only fuel resentment and hatred towards the U.S. and make it easier for our adversaries to plan and conduct asymmetrical attacks.

Chapter 1

Introduction

The purpose of this study is to investigate the effects of globalization on asymmetrical warfare in the next two decades and to recommend United States policy and force structure changes to deal with the evolving threat. Globalization has greatly increased the ability of adversaries to target the United States and other industrial nations using asymmetrical means. The benefits of globalization make it easier to use tools intended to bring the world closer together to commit asymmetrical attacks on our informational, economic, military, and political instruments of power. Additionally, the unifying vision of globalization often breeds resentment in underdeveloped nations by those who feel that they are being exploited by or not benefiting from this thing called globalization. While this phenomenon has gathered steam over the last decade, the world has not necessarily become the "Utopia" that many envisioned just a few years ago. Ethnic fighting in the Balkans and Africa, the failure of the Middle East Peace Process, the compounding world financial crises, the spread of disease, environmental calamities, and the rise of global terrorism have brought a new reality home to us. Just because the world is becoming more connected, does not mean that it is becoming safer, or even more tolerant of other cultures. What is clear, however, is that this thing we call "Globalization" has changed the world in which we live. It has created new possibilities

for nations and people to cooperate on a wide range of issues from trade, to humanitarian assistance, to the development of new technology.

The reverse side of this phenomenon is what we will explore in this research paper, globalization is not completely progressive and technology is morally neutral. The same tools being used to advance world societies and economies can also be used to help destroy them. Benjamin Barber describes a world that is both coming together and falling apart in his book *Jihad Against McWorld*. He describes a world where the nation state is losing its influence and where the world is returning to tribalism, regionalism, and the ethnocentric warfare that characterized much of the earlier human history[1]. While some dispute Barber's assessment, it is clear that globalization may be contributing to as many problems as it is solving. While the world is becoming more connected, it is not necessarily becoming better.

This problem is most apparent in the developing world where we continue to see the spread of disease, continuing humanitarian crisis, political and economic instability, and ethnic, tribal, civil, and drug related war. *Global Trends 2015* believes globalization will have a negative impact because of "the adverse affects of globalization and insufficient attention to reform"[2]. *Global Trends 2015* further offers four alternative global futures based on the effect of globalization.

There are several themes that are consistent across these global futures. The first is conflict. The negative effects of globalization will continue to promote regionalism, tribalism, and conflict in the developing world. Secondly, nations with uncontrollable population growth, a scarcity of natural resources, and poor government systems will fail to benefit from globalization regardless of its effects on the rest of the world. Thirdly,

technology will continue to be exploited to benefit developed nations and illicit criminal/terrorist networks, and will have little affect on the developing world. Finally, in all scenarios, U.S. power or global influence will lessen in relation to our ability to deal with both state and non-state actors [3]. In all scenarios the power of the state will weaken and the power of the non-state networked actor will continue to expand with the help of the tools of globalization.

As globalization continues to increase it will only widen the gap between the U.S. and the developing World. As this gap widens and information and technology continue to transfer to the emerging world, we are going to have to deal with better organized and equipped networked threats. This paper will examine how globalization is affecting this threat, and how the U.S. needs to organize in the future to deal with our changing environment.

Notes

[1] Barber, Benjamin, R, *Jihad Vs. McWorld,* Time Books, New York, 1995,3-6.

[2] *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, National Intelligence Council NIC 2002-02, December 2000, 5.

[3] Ibid, 43.

Chapter 2

Globalization, Information, and Power

Globalization has greatly increased the ability of adversaries to target the United States and other industrial nations using asymmetrical means. The same tools being used to advance world societies and economies are increasingly being used as tools to help destroy them. The events of September 11, 2001, are a perfect example of this trend. Nineteen Muslim fundamentalist terrorists from six countries entered the United States over a three-year period using reasons such as education, travel, and job training to gain initial entry into the country. Once in the U.S. they used the existing infrastructure (internet and telephone system) that was intended to promote idea sharing and knowledge to communicate securely with the sponsors of terrorism in places such as Pakistan, Saudi Arabia, Yemen, and Afghanistan. They were able to transfer over $500,000 from abroad to support the operation because our global financial network supports the transfer of $1.5 trillion a day to enable global trade and investment, and $500,000 is not enough to attract any attention.

Figure 1: Twin Towers

They then used another tool of globalization, the U.S. air transportation system that was intended to connect America with the rest of the world to attack the symbol of U.S. economic and cultural power, the twin towers of the World Trade Centers.

The series of coordinated attacks of September 11th demonstrate how globalization has increased the ability of terrorist and other non-state actors to project power in the global environment. In addition to simply causing terror, the attack resulted in billions of dollars worth of actual physical damage to the city of New York and the Pentagon in terms of real property lost, billions of dollars in lost business, and lost investment value. This does not include the cost of the War on Terrorism estimated at a billion dollars a month or the increased costs of homeland defense and future disaster preparedness. When coupled with the costs of the yet unattributed anthrax attacks, the asymmetrical attacks against the U.S. from September to December 2001 have cost more than the entire U.S. Defense budget of $365 billion allocated in FY 03[1]. Some estimates range as high as $2 trillion [2].

This encapsulates the main idea of this research paper--globalization has greatly increased the ability of both state (emerging countries) and non-state (terrorists, narco-

terrorists, criminal organizations) actors to project power on global scale. Globalization has directly contributed to the ability to inflict massive real damage to what has been called the world's last superpower. Moreover, it also demonstrated worldwide implications because economies are so globally connected. When U.S. airports shut down for three days, it affected every industrial nation in the world. When the U.S stock markets were closed, it had a tremendous negative effect on the world markets. Had the U.S. financial system collapsed, it is almost certain that world markets would have soon followed?

To further explain this connection, we will explore various definitions of globalization and its influences on the international landscape. There are two major schools of thought on globalization. The first is that globalization is a progressive movement that will only increase opportunities and raise the standard of living worldwide---or more simply that globalization is inherently good. As nations, cultures, and people interact with each other, they are bound to become more culturally aware, and more apt to cooperate and solve problems in a way that is more mutually beneficial to all.

The second school of thought is that globalization has further widened the gap between the have and have-nots of the world and that the information revolution simply allows the developed powers to flaunt this superiority on a global scale. The developed nations are not getting richer by helping the rest of the world develop through globalization, but rather by exploiting the developing world for their own benefit. We will examine these schools of thought in more detail below in order to analyze their effects on the rise of the global asymmetrical threat.

Globalization

In order to analyze globalization, we need to first agree on what globalization is. *Global Trends 2015* characterizes globalization as

> "…the rapid and largely unrestricted flow of information, ideas, cultural values, capital, goods and services, and people: that is, globalization". It further states "…governments will have less and less control over flows of information, technology, diseases, migrants, arms, and financial transactions, whether licit or illicit, across their borders. Non-state actors ranging from business firms to nonprofit organizations will play increasingly larger roles in both national and international affairs…. States with ineffective and incompetent governance not only will fail to benefit from globalization, but in some instances will spawn conflicts at home and abroad, ensuring an even wider gap between regional winners and losers than exists today." [3].

In *Jihad Against McWorld,* Benjamin Barber describes globalization as "McWorld", an environment "where by the onrush of economic and ecological forces that demand integration and uniformity and that mesmerize the world with fast music, fast computers, and fast food -- with MTV, Macintosh, and McDonald's, pressing nations into one commercially homogenous global network: one McWorld tied together by technology, ecology, communications, and commerce"[4].

In T*he Dark Side of Globalization*, the authors say "driven by an explosion in international productive and financial transactions, globalization implies a massive transition to a worldwide, free-market capitalist system. Transportation and information technology, twin pillars of modern capitalism, have fueled a complex world economy…"[5]. In *Unrestricted Warfare* the authors state, "The general fusion of technology is irreversibly guiding the rising globalization trend, while the globalization trend in turn is accelerating the process of the general fusion of technology, and this is the basic characteristic of our age" [6].

The insights above contain common elements that are critical to defining and understanding globalization. Those common elements are the explosion of people, capital and goods across international boundaries, the resentment and resulting ill effects caused by globalization, the increase and proliferation of information and technology, and the rise of non-state actor. These elements are critical in explaining the effect of globalization in relation to its impact on the asymmetrical threats facing the world in which we live. The explosion of people, capital and goods across international boundaries and resulting negative effects of globalization have been covered in some detail in chapter one and will not be expanded on in the coming chapters. These chapters will instead focus on proliferation of information and technology, and the rise of the networked actor that is being aided by globalization.

Information and Technology

The first factor is the rapidly changing role of information in all aspects of our society. Peculiar to this is that the information revolution has no ownership; it is a stateless revolution that is not controlled by a nation or nations. It is clear that the rapid transfer of information technology is having tremendous impacts on our society, but to what end is unclear. While it is evident that information is becoming universally available, it is less clear how that information will be used in the future. Is the proliferation of information good? Do people have a right to communicate secretly across borders? Does the general world population have the need to know the location of U.S. nuclear facilities, how to build WMD devices, our defense budget and major weapon system programs, or the travel itineraries of our major political and military leaders? The two areas of the information revolution we will focus on are information

technologies and the media and their effects on information dissemination.

In *The Changing Role of Information Warfare*, the authors explain that dramatic changes brought about by new information technologies are radically changing the world in which we live. These changes include large increases in international connectivity, access to the internet and to space-based communications and reconnaissance capabilities[7]. The information revolution has not only increased our ability to gather data, but it has greatly increased our ability to use that data on a global scale. The intent of the information revolution is that information is used for "the collective good", or to promote "prosperity " for all, but often times that is not the case.

The reality is that information availability is a double edge sword. It can be used to destroy just as easily as it can to build, to attack and to defend, and to exploit as well as protect, it is this perversion of the revolution that is critical to our understanding of the future threat. The only way for the technology to expand in its universal application and availability, this is also the way in which it is exploited. To expand on this, international global connectivity is needed to support global trade, finance, travel, and communication. In order for the network to support these tasks, it must provide global, secure and private means to communicate. The network provides this identical capability to potential adversaries as well as to legitimate interests. They can communicate, move finances, and plan operations utilizing the same tools as large corporations and states. The exploitation of the information revolution aided by globalization is having a tremendous effect on the ability of groups to organize, proliferate and act globally.

Media Effects

The second globalizing effect on information is the role that media plays in

influencing the world environment. The media has had a tremendous effect on a nations ability to pursue its national objectives in modern times. We saw the effects when the U.S. was forced out of Vietnam after the horrible images of the Tet offensive, out of Lebanon after the Marine barracks bombing, and out of Mogadishu after 18 Army Soldiers were killed and dragged through the streets.

In all of these situations it is clear what our adversaries were attempting to do, that is use the media to achieve objectives that were not attainable by military means. Did the death of 18 soldiers truly change the tactical balance of power on the streets of Mogadishu? Absolutely not, the U.S. military could have flattened Mogadishu after the incident, but the information battle was lost since any U.S. move would have been interpreted in an unfavorable manner by the world community and Americans at home. Public and international opinion allowed the Somali warlords to achieve through media what was military not achievable on the battlefield.

There are several other aspects of the media that are particularly difficult to manage. Media companies like CNN, Fox News, and the BBC exist for one reason, to make money. They do not work for and are not controlled by governments. They will report on a story if they believe it will cause viewers to watch. Most recently, we saw the effects of the Bin Laden videotapes that were broadcast worldwide. These tapes gave Bin Laden access to Muslims worldwide and allowed him to plead his case, condemn America and Britain, and call for further attacks. While the U.S. government was successful in keeping U.S. based media organizations from airing additional footage, Al Jeezera, the Qatar based Arab News Service, continued to broadcast the tapes. Al Jeezera broadcasted the tapes because it caused people to watch the news and that is the

essence of capitalism and globalism as it relates to the media. Governments do not control the media, but the media has demonstrated that it has an increasing ability to influence the actions of governments.

In the year 2020, it is projected that 13 of the 15 largest cities in the world will be located in Central/South America, Africa, South West Asia, and the Asia Pacific Region[8].

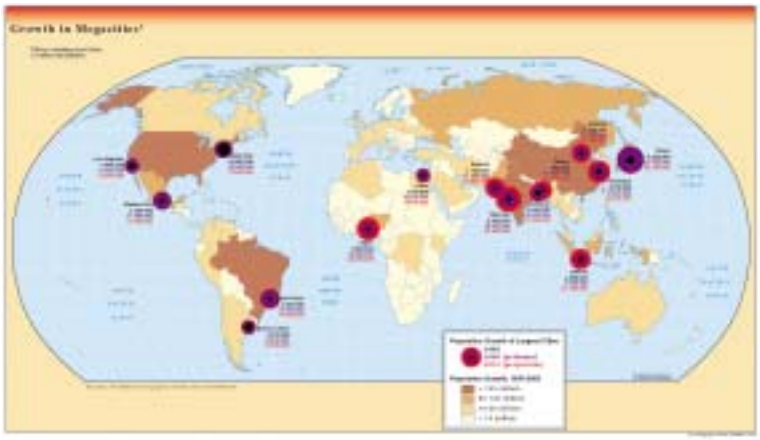

Figure 2: Growth in Megacities[9]

Additionally, of the 13, four are in are in India, three are in China, and two are in the Muslim countries of Pakistan and Indonesia. It is only logical that global news coverage will begin to cater more towards these areas as we continue to travel down the path of globalization. As globalization continues, the U.S. will lose its control of the major media outlets.

This means the U.S. will lose its hold on what some have called its "media howitzers". This excerpt from In *Athena's Camp below* outlines the effect media is likely to play in the future as globalization spreads.

> "…America's near-monopoly on media will not last. The "howitzers of the mass media," ... will not long remain the property …of the West. There are going to be Asian Rupert Burdocks and Muslim Ted Turners as the skies fill with private satellites ...mass media are still spreading into previously unfilled markets like Eastern Europe, Russia, and parts of Asia,

> the new media… include powerful new technologies that "de-massify" audiences and permit one-to-one customized communication. They also put cheap diffusion power in the hands of anyone with access to the Internet. …The Internet makes everyone a potential media producer on a global scale"[10]

The information revolution will continue to allow the disenfranchised populations of the world to exploit the belief that globalization is continuing to widen the gap between the western and developing world. As information technology spreads, and media markets broaden in the developing world, it will become increasingly difficult for western powers to mange the negative aspects of globalization and to prevent adversaries from exploiting the tools provided by information technology and media to assist in targeting western nations. Improved technology and the emergence of networked threats will only add to the effect of information in the global world.

Notes

[1] *Budget of the United States Government, Fiscal Year 2003*, February 4th, 2002, 101.

[2] Amberman, Christie, *Milken Institute Examines The Cost Estimates for Sept. 11th Attacks*, NGA Center for Best Practices, Washington D.C.

[3] *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, National Intelligence Council NIC 2002-02, December 2000, 6

[4] Benjamin, Barber Jihad Vs. McWorld *The Atlantic Monthly*; March 1992*;* Volume 269, No. 3; 53.

[5] *The Dark Side of Globalization*: United States Naval Institute Proceedings: Annapolis, NOV 2001, 1

[6] Liang, Qiao and Wang Xiangsui*, Unresticted Warfare*, PLA Literature and Arts Publishing House, Feb 1999. 6119

[7] Khalilzad, Zalmay, John White and Andrew Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare,* Defense Research Institute Report (Rand) 1999, 7-8.

[8] *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, National Intelligence Council NIC 2002-02, December 2000, 12.

Notes

[9] Ibid.

[10] Arquilla, John and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Defense Research Institute Report (Rand) 1997, xvii

Chapter 3

Technology Proliferation, and the Rise of the Network

"Technology has no conscience of its own"

—John F. Kennedy

Along with the first aspect of information and media, the second key aspect of globalization that is affecting asymmetrical capabilities of our potential adversaries is that of information technology advances, proliferation and transfer and the rise of the networked actor. Technology was once the weapon of the strong as the U.S. demonstrated with its overwhelming defeat of the numerically superior Iraqi Army during OPERATION DESERT STORM. The stunning defeat in less than 100 hours had many talking of the Revolution in Military Affairs (RMA) that had forever changed the ability of modern, technologically advanced nations to wage war. The debate still rages about whether we have had or are in an RMA, but what is increasingly clear is that the technology that enabled the U.S to defeat Iraq, is now becoming universally available.

Technology Transfer

Technology transfer has really taken three forms. First there is almost universal access to space-based imagery, the global positioning network, and worldwide secure communications network. Second, it is now extremely easy to purchase technologically advanced weapons such as GPS Jammers, Radio Direction Finding Equipment, night

vision devices and handheld radios at a fraction of the cost the U.S. paid to develop them. Finally, the cost of modern weapons has become so great, that it has increased the dependence on joint military and civilian ventures where technology transfer to the civilian community is increasingly difficult to control.

Spaced based imagery is now widely available on the internet, and commercial imaging companies now have access to U.S. military facilities worldwide. While this imagery does not reach the level of real time imagery available to U.S forces at the tactical level, it does provide a tremendous resource for someone who is planning an asymmetric attack. During a fifteen minute search on the internet one is able to obtain high quality imagery of Washington D.C., The Pentagon, several of our nuclear facilities, and almost any U.S. military installations. This information is available to anyone with a computer and a modem. If one is willing to pay, the information can be sent worldwide in near real time. If an adversary were planning an attack against a U.S. nuclear facility, this would provide an invaluable planning tool.

Figure 3: Imagery of Nuclear Facility[1]

Access to GPS systems, Satellite phones, and secure internet communications have

given criminal and terrorist networks access to the same level of information that was once available to only the most sophisticated nations. Terrorist groups and extremist organizations are making unprecedented use of this new technology as outlined in a report by the National Infrastructure Protection Center. "Extremist groups are increasingly adopting the power of modern communications technology. An extremist organization whose members get guidance from e-mails or by visiting a secure web site can operate in a coordinated fashion without its members ever having to meet face to face with other members of the organization."[2]

This new technology is facilitating in three major areas. First, the internet is being used to indoctrinate new members into terrorist/extremist organizations and bombard them with a steady stream of propaganda. This propaganda indoctrination can be conducted from a safe area where the leaders are free from any threat of law enforcement. Secondly, access to online communication sources like free e-mail accounts, chat rooms, and web-based bulletin boards, make it difficult to track where messages are coming from or going to. It provides a means for almost worldwide secure communication. The emergence of more sophisticated technology, like anonymous remailers, encryption, or steganography, will only make identification and tracking more difficult. Finally, internet gathering points such as Internet Relay Chat (IRC) or ICQ (I seek-you) allow dispersed members to share ideological and operational information, enabling them to centralize their shared world view into independently actuated agendas in support of a common goal [3].

Merging of Defense and Commercial Technologies

Another reality of the globally connected world is the merging of defense and

commercial technologies on a global scale. It is only logical that as our defense industries shrink and consolidate, they will have to produce products that have both military and civilian, dual use capabilities to survive. The ability to achieve competence in civilian production and defense-industrial applications is becoming increasingly inter-twined. At the same time, market access in the developing world (e.g. in East Asia) increasingly requires technology sharing as an instrument of commercial competition"[4]. The proliferation of weapons technology will be an increasing problem

> "Technology diffusion to those few states with a motivation to arm and the economic resources to do so will accelerate as weapons and militarily relevant technologies are moved rapidly and routinely across national borders in response to increasingly commercial rather than security calculations. For such militarily related technologies as the Global Positioning System, satellite imagery, and communications, technological superiority will be difficult to maintain for very long"[5].

The ability to purchase 3rd generation Night Vision Goggles (NVG) and laser aiming devices is a perfect example. The U.S. Army has said for years that they own the night, but one can purchase the same Night Vision Goggless worn by U.S. Special Forces for a fraction of the cost on the internet today. One can also buy Russian equipment using similar technology in bulk even cheaper and be assured that one will not have to worry about attracting the same amount of attention that a U.S. deal could possibly bring. Rogue nations, terrorist groups, or criminal organizations could purchase and employ this technology in order to negate the current advantage held by U.S. during night combat operations.

The Rise of the Networked Actor

The next aspect of globalization we will discuss is the rise of non-state networked actor. While this phenomenon includes the rapid proliferation of Non Governmental

Organizations (NGO), Private Organizations (PVO), and International Organizations (IO), we will primarily focus on terrorist and criminal networks. It is important to study these non-state actors because as Van Creveld writes

> "In today's world, the main threat to many states, including specifically the U.S., no longer comes from other states. Instead, it comes from small groups and other organizations, which are not states. Either we make the necessary changes and face them today, or what is commonly known as the modern world will lose all sense of security and will dwell in perpetual fear."[6].

The last 10 years have seen the rapid advance in networked terrorist and criminal organizations worldwide. This includes but is not limited to Al Qaeda who is said to operate in some 60 Countries, numerous terrorist/insurgent groups such as the Liberation Tigers of Tamil Elam (LTTE) and Hamas, Hizbullah, Islamic Jihad, Central, South American and Asian drug lords that operate networks spanning the globe, and a network of loosely connected smugglers that move contraband worldwide. While it is not clear to what extent these organizations are connected, it is clear that the lines between terrorist, drug smuggler, and insurgent are no longer easy to define. It is evident that Al Qaeda used the same networks to smuggle weapons drugs and money as it did to plan terrorist operations and that the Frente Armada Revolutionario de Colombia (FARC) in Colombia is financing an insurgency with money made selling and protecting cocaine shipments. The fact that several reported members of the Irish Republican Army have been killed or captured in Colombia, and that terrorist trained in Afghanistan are fighting in the Philippines, China, Indonesia, Somalia, Kashmir, and Algeria (to name a few) add another dimension to the inter-connected terrorist world. Pirates in the South China Sea have been caught transporting automobiles, drugs, people, weapons, and potential WMD material along their route. While the links are not clear, it is evident that these

enterprises are becoming more interconnected.

Global Trends 2015 summarizes the movement best

> "Criminal organizations and networks based in North America, Western Europe, China, Colombia, Israel, Japan, Mexico, Nigeria, and Russia will expand the scale and scope of their activities. They will form loose alliances with one another, with smaller criminal entrepreneurs, and with insurgent movements for specific operations. They will corrupt leaders of unstable, economically fragile or failing states, insinuate themselves into troubled banks and businesses, and cooperate with insurgent political movements to control substantial geographic areas. Their income will come from narcotics trafficking; alien smuggling; trafficking in women and children; smuggling toxic materials, hazardous wastes, illicit arms, military technologies, and other contraband; financial fraud; and racketeering"[7].

It is evident that as the nations of the world become more connected the criminal organizations that were once independents are doing the same. These organizations are developing three basic types of networks aided by the tools of globalization discussed above. Those types of networks are the chain or line network, the hub, star, or wheel network, and the all channel or full-matrix network [8].

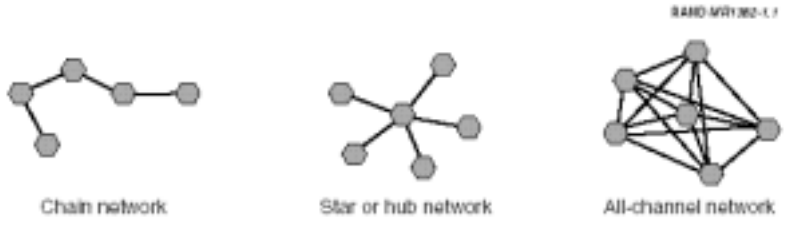

Figure 4: Types of Networks

These different network types and variants have allowed what were once local or at best regional terrorist organizations to expand operations on a transnational or global scale. Technology and the internet have allowed them to become globally netted players. The basic function of a network is relatively simple. A chain network is used when

goods or information move along a network or series of hubs until reaching a final destination. This type of network is normally used by pirates and smugglers where there is no central figure controlling the overall operation. The hub or star network is what we would normally recognize as a terrorist group, drug cartel or crime syndicate. In this case nodes operate separately, but must coordinate activities through a central node or leader. The all-channel network is a shared network of numerous groups loosely connected for a common cause.[9]

From a security standpoint, all of these network organizations present a difficult problem for us to counter. In all cases, destroying a node does not necessarily defeat or disable the network ability to conduct future operations. The second problem is that network nodes do not normally conduct an attack, but rather they provide resources that come together for a specific operation. In this case, terrorists from several nodes would come together to plan and conduct an operation, and then simply be absorbed back into the network environment. We are then fixed on finding this "Cell" that no longer exists but was brought together briefly and then immediately disbanded. In most cases the operatives will know very little about the final target, so if a member is compromised, he provides little actionable intelligence to Western agencies. This is the type of network we are dealing with in Al Qaeda attacks, and that the Israelis are dealing with in the case of Hamas.

The other significant fact about these networks is that globalization is providing the ability of a once local insurgent movement to organize and operate on a global scale. The LTTE in Sri Lanka is a perfect example. They have formed

> "a quasidiplomatic structure that consists of sympathetic pressure groups, media units, charities, and benevolent nongovernmental organizations

> (NGOs)... is especially reliant on electronic propaganda disseminated via the World Wide Web, news groups (Usenet), and email. These web sites have enabled the LTTE to establish a truly global presence, permitting the group to "virtually" and instantaneously transmit propaganda, mobilize active supporters, and sway potential backers... the LTTE runs a sophisticated international revenue-generating operation that draws heavily on Diaspora contributions…will siphon off contributions given to nonprofit NGOs, benevolent donor bodies, and other front organizations that finance Tamil social service, development, and rehabilitation programs in Sri Lanka….it is particularly difficult to prove that funds raised for humanitarian purposes are being diverted to propagate terrorism or other forms of illegal activity elsewhere."[10] .

This arrangement, or ones similar to it, are being repeated all over the world. In the Middle East we have seen the rise in what is being termed the "techno–terrorist"[11] Current operations in Afghanistan have uncovered a lot of details about the use of satellite phones, cell phones, faxes, computers, disks, and the use of the internet and e-mail to support current and plan future operations. Hamas is using the internet to plan operations, disseminate propaganda, and communicate with supporters abroad to include those in the U.S. This has also provided Hamas a secure communications channel across Gaza, the West Bank, and Lebannon. Hizbullah has used its three Internet sites to describe recent attacks and provide a constant source of news and propaganda. [12].

Group Name	Country of Origin	Web Address
Almurabeton	Egypt	www.almurabeton.org
Al-Iama'ah Al-Islamiyyah	Egypt	www.webstorage.com/~azzam/
Hizb Al-Ikhwan Al-Muslimoon (Muslim Brotherhood Movement)	Egypt	www.ummah.org.uk/ikhwan/
Hizbollah	Lebanon	www.hizbollah.org www.moqawama.org/page2/main.htm www.almanar.com.lb http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah/emdad
Hamas (Harakat Muqama al-Islamiyya)	Palestianian Authority	www.palestine-info.net/hamas/

Figure 5: Website examples

Irish Diaspora in the U.S. support the IRA through front organizations, Muslim Diaspora operate cells in North America, Europe and Asia to both raise money and plan attacks against western interests, and wealthy individuals and states continue to support known terrorist organizations. The terrorists and criminal networks are only going to become more networked and technologically savvy as information and technology continue to expand globally.

Information, media, and technology have radically changed the world in which we live. Adversaries have formed networks and utilized these tools to organize, recruit, and communicate securely on a global scale. Organizations that once maintained only the capability to act locally are now able to act internationally. This ability is only going to increase as globalization continues to quicken the transfer of new technologies, and as economic prosperity in the Western world continues to leave developing nations behind. Certainly the U.S. and its allies will have to deal with a better organized, equipped, and dangerous future threat.

Notes

[1] *Intelligence Resource Program*, Hanford Site Fast Flux Facility, 09 November 1978, Photo Number 094005001, http://www.fas.org/irp/imint/doe_hanford_fftf_01.htm

[2] National Infrastructure Protection Center, *Highlights 10-01,* November 10th 2001,2

[3] Ibid.

[4] Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, *CSIA Studies in International Security* No. 4, 1994, 47-48

[5] *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, National Intelligence Council, NIC 2002-02, December 2000, 31

[6] Van Creveld, Martin, In Wake Of Terrorism, Modern Armies Prove To Be Dinosaurs Of Defense, *New Perspectives Quarterly*, Vol. 13, NO 4, Fall 1996, 58.

[7] *Global Trends 2015*: *A Dialogue About the Future With Nongovernment Experts, Nationional Intelligence Counci*l NIC 2002-02, December 2000. 22.

[8] Arquilla, John and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute Report (Rand) 2001, 7-8.

[9] Ibid, 8-9.

[10] Byman, Daniel, et al. *Trends in Outside Support for Insurgent Movements*, Defense Research Institute Report (Rand) 2001, 44-51.

[11] Khalilzad, Zalmay, John White and Andrew Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare,* Defense Research Institute Report (Rand) 1999, 98.

[12] Ibid, 99.

Chapter 4

Asymmetrical Warfare and Threats to the United States

"Poorly paid, highly inebriated men make a shabby line of defense against terrorist and traffickers"

—Time Magazine

We have explored globalization and its negative effects in some detail. In particular, globalization has facilitated the ability to rapidly transfer information, money, ideas, and goods across international boundaries. It has assured that cutting edge technology once available to only the most powerful states can now be almost universally obtained. It has enabled any person or group to communicate securely across international boundaries and has supported recruitment and indoctrination for terrorist organizations. Finally, we talked about the fact that globalization has not lived up to its positive vision. Even though the world is more connected, we have not eliminated conflict, disease, or economic and political instability. The second part of this paper will analyze the asymmetrical threat that the U.S. and its allies will face in the coming years given the context described above. The paper will define asymmetrical warfare, identify how globalization will only increase the threat, and recommend U.S. policy and force structure changes to deal with the threat.

Asymmetric warfare has become increasingly important in the eyes of U.S. national security strategists since the end of the cold war. More U.S. citizens (both military and

civilian) have been killed or wounded by asymmetrical attacks in the last 20 years than by our conventional military involvement in Grenada, Panama, Desert Storm, Bosnia, and Kosovo (this is even before the attacks of 9/11)[12]. It is almost impossible to pick up the results of a study or survey, or listen to a major foreign policy speech in the last five years and not find reference to the asymmetrical threat facing the U.S. This was true even before the attack of September 11th. Since then it appears that the asymmetrical threat from terrorism will continue to be our number one national focus. In order to better understand asymmetric warfare, it is necessary to define what it is, and is not.

Asymmetrical warfare is in the simplest of terms "warfare that applies comparative advantages against an enemy's weaknesses[3]". This is not a new or particular revolutionary concept. The U.S. military attempts to engage in asymmetrical warfare whenever we meet an enemy on the modern battlefield. The U.S. military uses its comparative advantage in terms of technology, training, leadership, and ISR capabilities to attack what we perceive as our enemy's weakness. This has resulted in a series of one-sided campaigns in Iraq, Bosnia, Kosovo, and Afghanistan. This is precisely why it is becoming less and less likely that other states will attempt to engage us in a conventional conflict anytime soon. For this reason, both nations and non-state actors are increasingly relying on asymmetrical means to attack our interests. When used in this context, asymmetrical warfare focuses on the application of unconventional type weapons to achieve a desired outcome.

In the unconventional sense, asymmetric warfare is the ability to think and act in a manner that is not defensible with a conventional military force. Asymmetric attacks share certain characteristics that separate them from traditional military operations. First

groups or individuals that are not tied directly to a state normally conduct them. This makes detection and retribution extremely difficult. Secondly, the targets are not limited to military facilities or combatants, but rather a wide range of targets that have political, economic, and societal significance are attacked. The intent is to target an adversary's vulnerabilities. Thirdly, asymmetrical attacks seek to have a major psychological impact, an attack on one's will and ability to act or freedom of action. Finally, the methods used to conduct these attacks transcend what we would consider traditional even by terrorist standards. Recent examples include using airplanes, barge tenders, the U.S. Postal system, car bombs, and cyber systems as weapons.

What is clear is that these asymmetrical attacks are becoming more frequent, more creative, and increasingly more damaging. When we discuss asymmetrical attacks we must also consider cyber, nuclear, biological, chemical, and radiological attacks. While cyber attacks occur daily, we have only recently seen our first biological attacks with anthrax, and chemical attacks with sarin gas in the Japanese subway system. We see daily reports about rogue nations, terrorists, and criminal organizations attempts to get their hand on nuclear weapons. The threat is growing, globalization is helping, and it is only going to get worse.

Now that we have looked at globalization and defined asymmetrical warfare, we will examine the threat to the U.S. The following quote outlines the threat facing the US. in the next 15-20 years

> "most adversaries will recognize the information advantage and military superiority of the United States in 2015. Rather than acquiesce to any potential US military domination, they will try to circumvent or minimize US strengths and exploit perceived weaknesses. IT-driven globalization will significantly increase interaction among terrorists, narco traffickers, weapons proliferators, and organized criminals, who in a networked world

> will have greater access to information, to technology, to finance, to sophisticated deception-and-denial techniques and to each other. Such asymmetric approaches—whether undertaken by states or nonstate actors—will become the dominant characteristic of most threats to the US homeland"[4].

When we take into account the other negative effects of globalization, it is clear that organizations outlined above will have a large, economically depressed population to recruit from. Specific threats include increasingly destructive terrorist attacks against critical infrastructure targets in the U.S. and our overseas interests, cyber attacks, and attacks on military targets to prevent our ability to employ our technological superiority in combat.

Nuclear Terrorism and Critical Infrastructure

Nuclear terrorism is the greatest single threat the U.S. faces in the coming years. The events of September 11th have finally brought home the realization that the new super-terrorist organizations will use any weapon they can acquire to achieve the greatest possible effect in terms of casualties and real property damage. The myth that they would never use a chemical, biological, nuclear or radiation weapon simply holds no weight in the changed international environment. Recent information shows that today's terrorists will not only use such a weapon, but are actively seeking to obtain one. It has been reported that Russia has broken up over 600 criminal transactions involving atomic material since 1998, Turkey has disrupted over a 100, and countries all over the world have reported attempts by criminal networks to buy, sell, or transport atomic materials [5]. These transactions include both weapon and non-weapon grade nuclear material, and atomic waste that can be used in dirty bombs. With so many incidents being reported it is only logical to expect that some transactions may have been conducted successfully. It

is clear that international criminal organizations have the ability to interact with transnational terrorist organizations in that criminal/terrorist configuration that was discussed in chapter 3. It is only a matter of time before terrorist organizations attempt to detonate a rudimentary nuclear device in a U.S. or Western population center. This has to be the number one priority for the U.S. in terms of prevention of asymmetrical attacks. Terrorist organizations are extremely difficult to penetrate because religious ideology and fanaticism are often very difficult to fake. Criminal networks are somewhat easier because they exist to make money, and money often bends ones better judgement.

Terrorist attacks against critical infrastructure seem to be the most immediate threat in the near term. The FBI, CIA, and Secretary of Defense have recently commented on the intelligence gathered during Operation Enduring Freedom that points to operational planning by terrorist groups in Afghanistan. This includes attacks against nuclear power plants, water sources, and major transportation hubs. The bottom line is that as our national infrastructure becomes more dependent on technology for operation, it is going to become more vulnerable to our adversary's ability to conduct cyber and computer attacks. The Homeland Defense Force described below would form a key partnership with those responsible for security of our critical infrastructure to improve information sharing and threat preparedness.

Cyber Attack

Cyber attacks will both support and increase state and nonstate actor ability to inflict both hard and soft damage to U.S. targets. The ability of state and non-state adversaries to purchase state of the art computer systems will increase the already significant amount of cyber attacks against the U.S. As the U.S. becomes more dependent on computers for

both military and civilian applications, our adversaries will become more adept at using the computers we depend on as a tool to attack our economic, industrial, and military sources of power. Adversaries will increasingly use computer networks for attack because they represent an area where the comparative advantage of the U.S. is still relatively small. The other advantage of a cyber attack is that it can be conducted without fear of retribution. Imagine the international outrage if the U.S. retaliated against a state or non-state actor because they conducted a cyber attack against the Pentagon? Often times cyber attacks allow you to commit acts of war without revealing what nation or organization the attacker is affiliated with. It is the perfect attack in the asymmetrical since because it allows the weak to attack the strong with very little fear of retribution.

Military Threat

The U.S. Military is not going to be confronted in a conventional manner anytime soon. Desert Storm, Allied Force, and Enduring Freedom have demonstrated that it is simply not possible to oppose our military might in a conventional sense. Adversaries have almost no chance to shoot down our aircraft, oppose our ground forces, or prevent us from maneuvering at will on the battlefield. What we are going to see in the future, are attacks against our key facilities, staging bases, and networks that are more vulnerable and less protected than forces once involved in combat. It is probably easier to infiltrate and destroy a B2 Bomber on the ground at its home base than in the sky over a target. It is invisible in the air, but not on the ground. An asymmetrical warrior will not necessarily try to destroy the combat platform, but he will try and destroy the only factory that produces the JDAM, or the air refueler fleet that allows the bomber to accomplish the mission but is guarded by much less security. This is the threat of the

future, the adversary will attempt to negate the combat capability by identifying and attacking the weakest link in the system. This adversary will jam our GPS guided bombs, attack our communications networks, and attempt to sway international opinions by using the media and internet to plead their case.

Notes

[1] U.S. Department of State, *Significant Terrorist Incidents 1961-200*, Office of the Historian, Bureau of Public Affairs, October 2001, 2-9.

[2] "Post Vietnam Combat Casualties", *Infoplease.com,* Learning Network, 2002, http://www.infoplease.com/ipa/A0778300.html.

[3] Dunlap, Charles, Lecture to Air Command and Staff College, Maxwell AFB AL.

[4] *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, National Intelligence Council, NIC 2002-02, December 2000,9.

[5] Jeffrey Kluger, The Nuke Pipeline" *Time Magazine,* November 26, 2001, 40.

Chapter 5

U.S. Force Structure and Policy Changes

> *Global terrorist activity is one of the by-products of the globalization trend that has been ushered in by technological integration… Compared to these adversaries, professional armies are like gigantic dinosaurs which lack strength commensurate to their size in this new age. Their adversaries, then, are rodents with great powers of survival, which can use their sharp teeth to torment the better part of the world"*
>
> — Liang Qiao and Wang Xiangsui in Unrestricted Warfare

If the trend in asymmetrical attacks is the greatest threat facing the U.S., and is being fueled by the effects of globalization, then we must develop a security structure to deal with the threat. We must also address policy issues that continue to create animosity towards the U.S. and our allies in most of the developing world. The U.S. military force structure is little changed since the end of the cold war. While we have seen two Quadrennial Defense Reviews (QDR) and two Global Vision Documents, neither has included concrete force structure changes to deal with the threat. While we continue to talk about transforming the military, we have not linked that transformation to a desired set of capabilities that enable us to deal with the changing threats we face as globalization continues. We suffer the same problems when we are dealing with the other key players in our national security architecture. The CIA, NSA, NRO, et al, have suffered the same fate as the DOD, they have gotten smaller, but not better organized to deal with the changing threat.

DOD Force Structure

The current architecture of five regional and four functional Commanders in Chief (CINC) is not suited to deal with the threat of asymmetrical warfare that we face. It does not provide us the needed security from either a geographical or functional perspective and fails to leverage available information and information systems in a networked manner. For example, a group of computer hackers operating from Pakistan conduct a cyber attack against air traffic control radar at Los Angeles International Airport in the middle of an extreme weather situation. The air traffic controllers are unable to maintain adequate control of all inbound aircraft, several jets crash, the resulting shutdowns and fears across the airline industry cause hundreds of millions of dollars worth of damage. This was an attack against the U.S. from terrorists in the CENTCOM AOR, directed against an area owned by JFCOM (or PACOM). Who was/is responsible for preventing such an attack? The military does not have jurisdiction within our borders, so was it the FBI? The FBI is focused on the domestic not the international threat, so is it the CIA? It involved airplanes so was it the FAA, NTSB? No one really knows, and if we find the perpetrators, what can we do about it? Our current system simply is outdated and not prepared to deal with the current or future threat.

The system (predominantly military but includes non DOD agencies involved in national defense and law enforcement) is not prepared to deal with the networked based threat because it is a strict hierarchy that has developed over time based on very stringent rules and guidelines. In military organizations, orders flow down the chain of command while information required for decision-making flows up from subordinate units. While this type of organization proves particularly useful in fighting similarly organized forces,

it has proven inept at fighting the types of networks discussed in Chapter 3. The CIA and other civilian agencies are also similarly organized. The situation is further complicated by the fact the communication between the hierarchies (military to civilian or civilian to civilian) is often only allowed at the highest level. What we have then is a non-networked collection of military and civilian agencies that are organized in a hierarchal fashion and are responsible for preventing asymmetrical attacks against U.S. interests by networked terrorist and criminal organizations. The inability to stop the flow of drugs into the U.S., the failure of the Colombian military against the FARC, and the lack of success in stopping Hizbullah and Hamas in the Middle East are just a few examples of how similarly organized hierarchies have failed to prevent networked threats from achieving their objectives. Defense, law enforcement and national security related hierarchies are very good at fighting other hierarchies, but they are no longer the greatest threat. These hierarchies must network both nationally and globally to take advantage the opportunities globalization has created to share and transfer timely and accurate information.

Homeland Defense Force

There has been much speculation that the U.S. Military will establish a new CINC that has the specific responsibility of homeland defense. Recent news stories have mentioned a "Northern Command" that will be some sort of combination of NORAD and JFCOM under a new four star Commander In Chief. A homeland defense command will only sufficiently meet the current threat if it is a radically different organization that is organized more like the networked threat it is intended to prevent than like our current hierarchal organizations. As currently proposed, it does not appear that a "Northern Command" will be up to this task. It appears we are really just going to add the job of

homeland defense to the plate of CINC NORAND and give him a more prestigious title. This organization will not be suited to prevent asymmetrical attacks, and will keep CINC NORAND from his most important job, which is ICBM early warning, destruction and counter-attack. An organization as outlined below will be better suited to deal with the requirement of homeland defense.

The United States already has a Homeland Defense Force. It consists of the Coast Guard, National Guard, FBI, CIA, Border Patrol, Customs, DEA, Local Police, etc. It also consists of National Guard Weapons of Mass Destruction Civil Support Teams (WMD-SCT), Marine Corps 4th Marine Expeditionary Brigade, and Air Force Units flying CONUS CAP missions. Representatives of these agencies/forces should be brought together under the umbrella of homeland defense and the United States Military. The active Military should provide resources, command and control (people and facilities), and operational expertise. The primary weapon in homeland defense is not going to be the aircraft carrier, or a missile shield. The primary weapon is going to be information. The homeland defense force needs to be a network that facilitates the rapid transfer of information nationally and internationally to prevent attacks on the U.S. homeland, our citizens, possessions, forces abroad, and our friends and allies. Homeland Defense Forces should be computer, intelligence, crime, WMD, and industry experts. If a threat is located, we have forces highly trained to eliminate that threat. Our problem has not been the ability to destroy the threat, but gaining actionable information prior to the attack.

The Homeland Defense Force should consist of a network of Operating Locations dispersed nationally and internationally to leverage information to identify threats,

provide actionable intelligence to military commanders, provide public warning and crises response, and act as a national and international information coordination center. This Homeland Defense Force would not be responsible for combat air patrols over the nation, a missile defense shield, or physical security in terms of people and operational deployments. The U.S. already has forces and redundant command and control structures that can do these things, another layer of beaucracy will only make us less not more efficient.

As mentioned above, Operating Locations should be dispersed nationally utilizing existing infrastructure of national agencies, local agencies, and the reserve and active military components. In some cases an Operating Locations may consist of one or two people, in other cases we may be talking about 20 or 30, but what we need to avoid is placing another 1500 people in the D.C. area doing essentially the same thing that is already being done by numerous military and civilian agencies, special task forces, and working groups. There would of course be Operating Locations at key existing agencies to include the CIA, NSA, NRO, FBI, DEA, DOE and NORAD to capitalize on the existing infrastructure to collect and disseminate information.

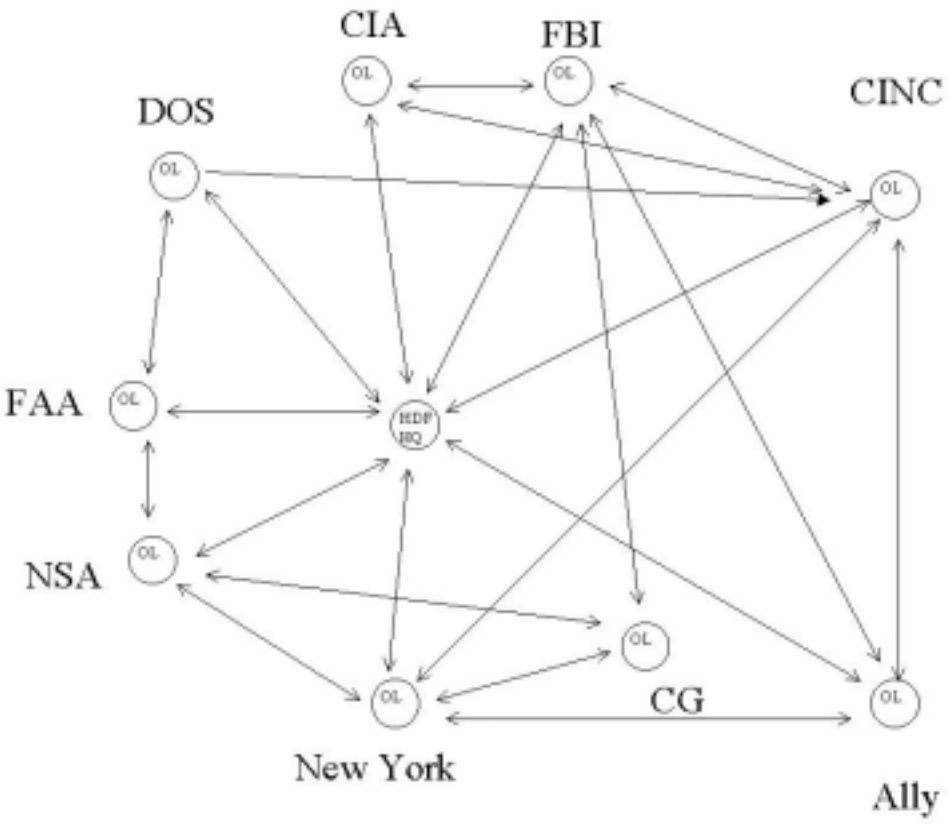

Figure 6: Sample HDF Structure

There would also be Operating Locations at key Coast Guard, FAA, Border Patrol, Customs, and INS to analyze information on who and what is getting into our country. Operating Locations would exist at the headquarters of regional and functional CINCs to provide liaison and expertise and to tie into the existing infrastructure for indications and warning. Operating Locations would be collocated with local police and emergency response forces in our major urban areas to share information, gather intelligence, and provide expertise. Operating Locations would also be positioned globally to provide liaison and share information that pertained to threats against civilized nations. This would include countries such as China, Russia, Pakistan, and Yemen and about everyplace else where the U.S. is allowed to operate. The bottom line is to deny

information safehavens just as we deny physical safehavens. The most productive arrangement would allow Operating Location in a foreign country to tie in to their network that essentially provides the same conduit for information within that country as outlined under the U.S. structure.

A sample Operating Location would consist of a mix of military and civilian experts whose job is to gather and analyze information to identify threats to the homeland. This civilian/military mix would allow the collection of information and apprehension of U.S. citizens posing a threat to the homelands under the auspices of existing civilian agencies and not require the suspension of Posse Comitatus within U.S. borders. If a threat is identified that requires military type force, it is immediately passed to the Operating Location at the appropriate military force headquarters, law enforcement agency, or foreign government for immediate action. Information would also be recorded in a database that could be queried for information from any Operating Location. They key here is to create an all channel network to gather, analyze and report information. The Operating Locations would not be hierachial in structure. We would not expect the HDF HQ to collect and analyze all information before forwarding to field locations for action. This is how our current system operates and it has not been very successful. In most of the major terrorist attacks in the last 10 years there have been indicators that were in the hands of U.S. intelligence prior to attacks that simply were not properly analyzed until after the attack. The case of Zacarias Moussaoui is a perfect example.

Zabib Zacarias Moussaoui was arrested three weeks before the attack on September 11th because the FBI was notified of suspicious activity by a flight school he had enrolled in and paid $8,000 to learn to fly commercial jets. The FBI detained him on immigration

charge until the September 11th attacks when the FBI started to piece together the puzzle. As it turns out, a wealth of information was available but not properly analyzed by the FBI. Moussaoui was already suspected of association with fundamentalist terrorist groups by French intelligence, was carrying the phone number to radical Al Qaeda Cell in Hamburg that included Mohammed Atta, and had been sent two wire transfers for $14,000 from that same cell[1]. The information was there, our system was just not set up to exploit it. Under the HDF structure outlined above, the Operating Location in Minnesota would have been notified when a Foreign National was arrested for the suspicious behaviors noted above. While the FBI worried about search warrants and constitutional rights (which took up most of their time in this situation), the local Operating Location would comb the network for information. He would contact the Operating Location at the FAA to see if there had been similar or unusual activity in any other flight schools and the Operating Location in London and France to research Moussaoui history and acquaintances. It would not have taken a tremendous amount of work to identify and prevent this attack before it occurred, but our system just is not set up that way. The current system does not facilitate to flow of information, networks do, and that is why they are becoming increasingly effective at attacking our interests.

Policy Issues

As discussed in this paper, globalization is greatly increasing the ability of potential adversaries to target U.S. interests on a global scale. The U.S. must take steps to ensure that our policies make it more difficult for potential adversaries (state and non-state) to acquire weapons and technology, attract recruits, and exploit poor security in developing nations. U.S. policy in each of these areas needs to be designed to defeat potential

adversaries before they act.

As stated earlier, the greatest threat facing the U.S. is that a terrorist organization will acquire an atomic device and detonate it in a major U.S. population center. As discussed, the criminal and terrorist networks necessary to steal, transport, and detonate such a device exist, are globally connected, and are becoming more technologically savvy. The events of September 11th demonstrate that high casualties are no longer not a concern, but rather the goal of organizations like Al Qaeda. The U.S. must take steps to stem the flow of WMD material. First of all, the U.S. must place more emphasis on the current program to secure nuclear facilities in the Former Soviet Union. That Program has been cut 40% since the Bush Administration took office[2]. A Czech citizen who was part of a group of uranium smugglers arrested near Munich in 1994 told *Time Magazine* that obtaining nuclear material from Russia was "like going for vacation by the sea and bringing back a sack of shells"[3]. The only way to prevent an attack with 100% certainty is to prevent the nuclear material from getting on the market, this must be the goal of the U.S. program.

The second step the U.S. must take is to prevent nuclear weapon proliferation to rogue sates. This includes but is not limited to Iran, Iraq, and North Korea. The U.S. must take an active versus reactive stance in ensuring these countries do not proliferate nuclear material. In the case of Iran and Iraq preemptive military action is probably necessary to prevent this proliferation. In North Korea, a policy that rewards North Korea and provides economic incentives is probably a better policy to follow. The U.S. must also put pressure on China, Russia, and France and to ensure that they do not provide technologies to these countries that have may have dual use capabilities.

Finally, the U.S. must attack the criminal network that trades in WMD material. As noted in Chapter 3, trafficking of nuclear material has become a common occurrence with hundreds of cases being reported annually. The current U.S. intelligence structure is overwhelmingly oriented towards collecting and analyzing military related intelligence. The U.S. must refocus its intelligence resources to identify criminal organizations that are involved in smuggling materials that can be used in these potentially devastating attacks. The U.S. Navy must increase its presence in key trafficking areas. The U.S. Coast Guard, Customs, and Border Patrol must be augmented to ensure that the U.S. can prevent entrance of these materials into the U.S. While this is not a traditional military role, it must be performed if we are to defeat this new threat.

The current policy concerning support to nations fighting terrorism within their borders should be maintained and expanded. Recent events have shown us that we simply cannot wait for an adversary to act and then retaliate, the losses are simply unacceptable. If countries have become safe-havens for terrorists, narco-terrorists, or criminal networks proliferating WMDs, then the U.S. must support host nation forces in their efforts to eradicate those forces. If host countries are unwilling or unable combat such forces, then the U.S. and its allies must act preemptively. If diplomatic or economic coercion (loan denials, sanctions), works, great, but if not we must be prepared to act militarily. The counter-argument to this is that we simply do not have enough forces, and that the U.S. would alienate our "coalition partners" if it acted unilaterally. While these operations put a strain on military forces, the U.S. does maintain enough forces to conduct worldwide operations and punish nations who would proliferate WMDs, export terrorism, and provide safe havens for potential adversaries. It does not make tactical

sense to wait for an adversary to develop and deploy a capability before acting. While direct U.S. action causes short-term alienation, it promotes long-term security and addresses the threat caused by global terrorists.

U.S. troop deployment in Southwest Asia and our policy in the Middle East continues to create an extreme amount of animosity towards the U.S. in the Muslim world and makes it easier for Islamic terrorists to find recruits, funding, and motivation necessary to conduct asymmetrical attacks against U.S. interests. The long term stationing of U.S. troops in Saudi Arabia is clearly a case where the cure has become much worse than the disease. The U.S. needs to act immediately to affect a regime change in Iraq and redeploy the bulk of our forces to less controversial locations. While this will cause some short-term problems with our Arab friends, it will greatly reduce the threat our long-term presence is having.

The Arab world views the U.S. as pro-Israel. This view continues to fuel resentment and pumps money and recruits into the coffers of Al Qaeda and Islamic Jihad. The most recent U.S. approach has been to let Israel and the PLO sort it out; this policy has clearly failed. We have once again allowed Muslim fundamentalists to wield a disproportionate amount of power in the Middle East. The U.S. must leverage its considerable influence in the region to force the Israelis and Palestinians to reach a workable agreement. If this issue is not resolved, it will continue to act as a flashpoint for local and international terrorist attacks[4].

The U.S. must examine its policy toward the developing world. Afghanistan showed the world what could occur when we allow a failed state to fester for a decade before acting. Is the next location Somalia, DROC, Zimbabwe, no one knows? The U.S. needs

to work both unilaterally and through organizations like the UN to prevent the collapse of failing states, and to rehabilitate those states that can no longer control what occurs within their borders. While no one wants to see the military deployed more to support humanitarian operations, we have to address problems within the developing world or globalization will ensure that those same problems are eventually exported to the U.S.

Notes

[1]Sarah Downey, "Who is Zacarias Moussaoui" *Newsweek Web Exclusive*, December 14th, 2001, 1-4

[2] Jeffrey Kluger, "The Nuke Pipeline" *Time Magazine,* November 26, 2001, 45

[3] Ibid, 44.

[4] Ian O. Lesser, "Strike The Roots of Terror", *Full Alert An Arsenal of Ideas for the War Against Terrorism,* Rand Report 2002

Chapter 6

Conclusion

This report has investigated globalization and its effects on asymmetrical warfare in the coming decades. Globalization has greatly increased the ability to target the United States and other industrial nations using asymmetrical means. The benefits of globalization make it easier to use the tools intended to bring the world closer together to commit asymmetrical attacks. Those key tools of globalization are information and technology. Globalization has also created an enormous gap between the developed and underdeveloped world that only fuels the rage of those who intend to cause us harm. The U.S. needs to reexamine its structure for homeland defense and change or reinforce current foreign policy initiatives to deal with this threat.

Information is the economic capital of a globalized world. It has been said that the amount of information available for world consumption doubles every 18 months. The technology that allows this information to be consumed internationally is now also available to worldwide terrorist and criminal organizations. They are using these informational tools of globalization to organize, communicate, and act. They are using media to include broadcast, print, and internet to bombard their faithful with propaganda and news about their cause. The information revolution has clearly enabled these organizations to influence the global environment.

Technology has always been the favorite tool of the powerful state actor, this is changing. Globalization has fueled technology proliferation and transfer on a global scale. Computer, global positioning and high tech weapon technology can now be purchased both legally and illegally worldwide. Terrorist and criminal organizations will continue to leverage this technology to conduct increasingly devastating attacks against the U.S. and our allies. The U.S. is not going to prevent the proliferation of this technology, instead it needs to adapt its force structure to deal with the evolving threat.

Globalization is not creating one homogeneous world moving down the road to economic prosperity and cultural enlightenment. Globalization is creating new problems as fast as it is solving old ones. Disease, natural disaster, wars, and global terrorism and crime continue to plague the world. U.S. foreign policy must address these issues and ensure that we do not allow the creation of additionally training and recruitment ground for the global terrorist and criminal threat.

The U.S. will continue to face threats to its national security as globalization exerts greater and greater pressure on the world. This threat includes asymmetric attacks against our population centers with weapons of mass destruction, against our critical infrastructure, our facilities abroad, and our military. The proliferation of WMD material to actors who wish to do us harm is the greatest single threat facing our country and should be given the highest national priority. The U.S. must work effectively with the Former Soviet Republics to prevent the proliferation of nuclear material. We must not allow rouge nations the ability to develop and export WMD weapons and material. In order to deal with the threat the U.S. must make organizational and policy changes.

The U.S. must take advantage of the network design if it is going to be successful in

dealing with and defeating the network threat we are up against. The problem is not the lack of forces or resolve, but the lack of actionable intelligence to prevent an attack. The U.S. should form its Homeland Defense Force around a network that is designed to leverage information in the information age. We should take advantage of the existing federal and local infrastructure to aid this organization but remain free of the bureaucratic layering that makes them ineffective as an information force.

The U.S. needs to focus its foreign policy to resolve the longstanding issues that only fuel hatred against the U.S. and provide flashpoints for terrorism, war, and criminal activity. We must also address failing and failed states to ensure that we prevent future Afghanistan from acting as training and recruitment areas for terrorists and criminals.

Globalization has changed the world. The effects of globalization are only going to increase as the world becomes more connected and dependent. As these effects increase, global terrorist and criminal networks will continue to exert greater influence in the international environment. The U.S. must make significant policy and force structure changes to protect its interests in a changing world. Those changes will allow the U.S. to positively deal with the negative aspects of globalization that provide our adversaries with opportunities, to take advantage of networked organizations made possible by the information and technology revolution, and to ensure the homeland is protected against asymmetrical attacks to the greatest extent possible.

Bibliography

Amberman, Christie, *Milken Institute Examines The Cost Estimates for Sept. Attacks*, NGA Center for Best Practices, Washington D.C.

Arquilla, John and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute Report (Rand) 2001

Arquilla, John and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Defense Research Institute Report (Rand) 1997

Barber, Benjamin, R*,* Jihad Vs. McWorld *The Atlantic Monthly*; March 1992*;* Volume 269, No. 3; pages 53-65

Barber, Benjamin, R*, Jihad Vs. McWorld,* Time Books, New York, 1995.

Byman, Daniel, et al. *Trends in Outside Support for Insurgent Movements*, Defense Research Institute Report (Rand) 2001

Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, *CSIA Studies in International Security* No. 4, 1994

Global Trends 2015: A Dialogue about the Future With Nongovernment Experts, National Intelligence Council NIC 2002-02, December 2000.

Ian O. Lesser, "Strike The Roots of Terror", Full Alert An Arsenal of Ideas for the War Against Terrorism, Rand Report 2002

Jeffrey Kluger, The Nuke Pipeline" *Time Magazine,* November 26, 2001, 40

Kennedy, John F, quoted in *Time,* November 26, 2001

Khalilzad, Zalmay, John White and Andrew Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare,* Defense Research Institute Report (Rand) 1999

Liang, Qiao and Wang Xiangsui*, Unresticted Warfare*, PLA Literature and Arts Publishing House, Feb 1999.

National Infrastructure Protection Center, *Highlights 10-01,* November 10th 2001

"Post Vietnam Combat Casualties", *Infoplease.com,* Learning Network, 2002, http://www.infoplease.com/ipa/A0778300.html

Rowley, Bill, RADM, The Future is not What it used to be, April 1995

Sarah Downey, "Who is Zacarias Moussaoui" Newsweek Web Exclusive, December 14th, 2001, 1-4

The Dark Side of Globalization: United States Naval Institute Proceedings: Annapolis, NOV 2001

U.S. Department of State, *Significant Terrorist Incidents 1961-200*, Office of the Historian, Bureau of Public Affairs, October 2001

Van Creveld, Martin, In Wake Of Terrorism, Modern Armies Prove To Be Dinosaurs Of Defense, *New Perspectives Quarterly*, Vol. 13, NO 4, Fall 1996